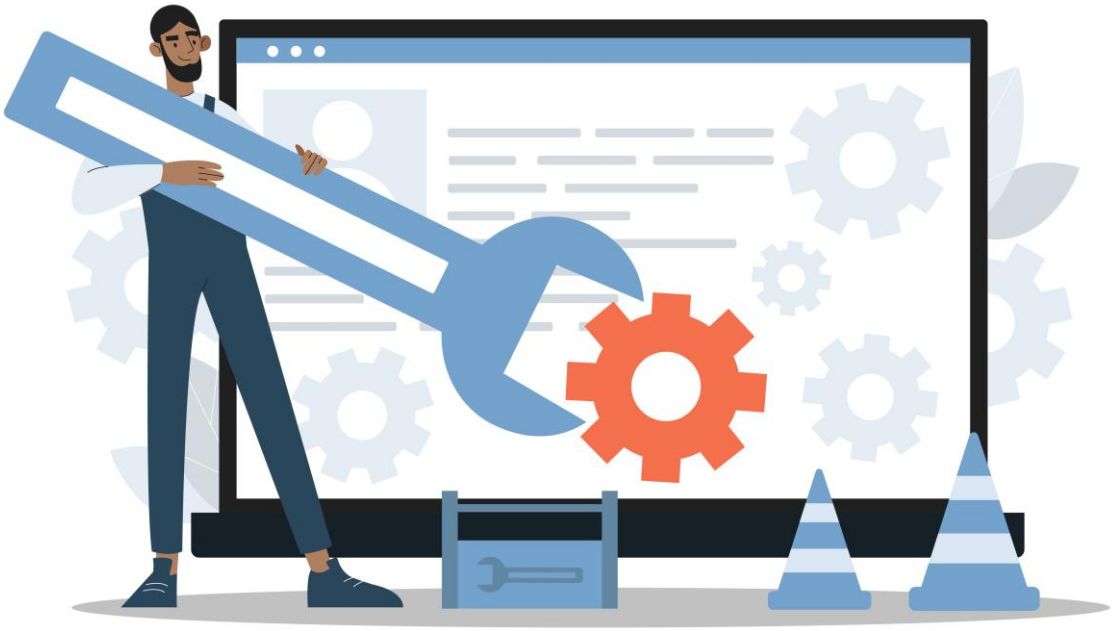

Podstawy Hardeningu

LEKCJA 1 – „Kto może wejść? – MAC Filtering, NAC i Access Control Lists”

1 | Cele lekcji

Po 45 minutach uczeń:

1. odróżnia **MAC Filtering** od **Network Access Control (NAC)**;
2. zakłada i testuje prostą **ACL** blokującą ruch do wskazanego hosta;
3. zapisuje decyzję „kto / co / kiedy” w szablonie dziennika zmian.

2 | Czas trwania

45 min

3 | Potrzebne materiały

Co	**Dlaczego / wersja awaryjna**
1 switch lub router (realny **lub** Packet Tracer)	pokaż tablicę MAC i ACL
Laptop nauczyciela (konsola)	konfiguracja na żywo
Laptopy uczniów (klienci)	test pingu / logowania
Arkusz „Dziennik zmian ACL” (wydruk)	notatki z adresami MAC/IP
Tablica lub flipchart	wizualizacja różnic

4 | Przebieg zajęć

Faza	**Czas**	**Co mówi / robi nauczyciel**	**Co robią uczniowie**
Wstęp	**5'**	**Wyświetl zdjęcie bramki stadionowej. „Sieć to impreza z biletami. Jak**	**Burza krótkich odpowiedzi; zapisujesz słowa-klucze.**

		decydujemy, kogo wpuścić?”	
MAC Filtering	8'	1️⃣ Pokaż tabelę MAC (show mac-address) i dopisz regułę „drop” dla jednego z laptopów ucznia (symulacja). 2️⃣ Wyjaśnij spoofing: łatwo zmienić MAC, więc metoda dobra tylko w sieci lokalnej.	Odczytują swój MAC (ipconfig /all lub ip a) i sprawdzają, że filtr działa.
NAC-based	10'	Krótka prezentacja portalu NAC (darmowy ClearPass demo / Packet Tracer): role „uczeń”, „gość”. Podkreśl: tu liczą się *uprawnienia* przypisane do tożsamości, nie sam adres.	Logują się do portalu, widzą inne VLAN-y / dostęp stron.
ACL	15'	Przeskocz na router. access-list 101 deny tcp any host 192.168.50.23 eq 80 access-list 101 permit ip any any int g0/1; ip access-group 101 in Opisujesz kolejność reguł i różnicę „in/out”.	W parach wymyślają 2 własne reguły (np. blok gier, blok torrent). Wpisują je w arkusz + uzasadnienie.

Podsumowanie	**7'**	**Na tablicy rysujesz tabelę:**	**Kryterium**

5 | Pytania do dyskusji

1. Kiedy MAC Filtering ma sens mimo możliwości spoofingu?
2. Co jeśli użytkownik nie przejdzie uwierzytelnienia NAC, a i tak trzeba mu dać Internet (np. gość-prelegent)?

6 | Ratunkowe wskazówki

- **Sprzęt nie wspiera ACL** → użyj Packet Tracer, a komendy wpisz w symulator.
- **NAC demo nie działa** → pokaż screenshoty portalu + szybkie Q&A o rolach.

7 | Dodatkowe źródła

- Cisco Packet Tracer „ACL Lab” (pliki *.pkt* do pobrania).
- Krótki film YouTube https://www.youtube.com/watch?v=gtZUHYvRFUY

LEKCJA 2 – „Zatkaj dziurę – Port Blocking i DNS Sinkhole”

1 | Cele lekcji

Uczeń:

1. Konfiguruje regułę firewalla (iptables / Windows Firewall) blokującą konkretny port.
2. Wskazuje różnicę między *drop* a *reject* oraz mierzy skuteczność (nmap, netcat).
3. Tworzy **sinkhole** dla złośliwej domeny w pliku *hosts* lub na lokalnym DNS.

2 | Czas trwania

45 min

3 | Potrzebne materiały

Narzędzie	**Zastosowanie**
VM Linux lub laptop z WSL	iptables
Port-listener (nc -l 6666)	symulacja malware
nmap, netcat, curl	testy
Kopia pliku *hosts* lub BIND / dnsmasq	sinkhole
Arkusz „Log testów”	notatki port-scan przed/po

4 | Przebieg zajęć

Etap	Czas	Instrukcje	Działania uczniów
Wstęp	4'	Story: „Zainfekowany host słucha na 6666/TCP i ściąga komendy z bad.example.com”.	Stawiają hipotezy blokady.
Blokada portu	12'	Demonstruj: sudo iptables -A INPUT -p tcp --dport 6666 -j DROP. Pokaż różnicę DROP vs REJECT.	nmap -p 6666 <IP> przed/po → wpisują czasy i wyniki do arkusza.
Sinkhole DNS	10'	Edytuj /etc/hosts: 127.0.0.1 bad.example.com. Wyjaśnij: ruch	curl http://bad.example.com → błąd. Zapisują co widzą w

		zostaje zlogowany lokalnie, nie wypływa.	/var/log/apache2/access.log .
Testy „Ciepło/Zimno”	14'	Ukryj, które porty blokujesz / odblokowujesz. Uczniowie mają 3 rundy skanu i raportu.	Analizują wyniki, szukają wzorca.
Podsumowanie	5'	“Zatkanie” ≠ “cisza”: sprawdzaj logi!	Wskazują min. 2 metryki skuteczności (brak ruchu, wpis w logu).

5 | Pytania do dyskusji

- Po co używać sinkhole, skoro można *dropnąć* domenę na firewallu?
- Jak pasować reguły portów, żeby nie zablokować legalnej aplikacji?

6 | Ratunkowe wskazówki

- **Brak uprawnień root** → netcat i firewall na lokalnym Win 10 (netsh advfirewall).
- **Nie działa DNS** → restart systemd-resolve lub ipconfig /flushdns.

7 | Dodatkowe źródła

- SANS Whitepaper „DNS Sinkhole 101”.
- man iptables – sekcja *Target Extensions*.

LEKCJA 3 – „Łataj mądrze – Patching i Group Policy”

1 | Cele lekcji

Po 45 minutach uczeń:

1. Klasyfikuje łatkę jako krytyczną / istotną / kosmetyczną.
2. Tworzy **GPO** wymuszające silne hasło i automatyczny lock screen.
3. Przedstawia plan rollbacku, gdy aktualizacja powoduje awarię.

2 | Czas trwania

45 min

3 | Potrzebne materiały

Co	**Uwagi**
VM z Win Server 2019 (AD) lub lokalny gpedit.msc	musi być lokalnie dostępny
Lista świeżych biuletynów CVE (wydruk)	dyskusja krytyczności
Arkusz „Cykl patchowania”	fazy test → prod
Flipchart / tablica	wizualizacja

4 | Przebieg zajęć

Segment	Min	Co robisz	Co robią
Intro CVE	6'	Pokazujesz CVE-2023-XXXX (RCE) na slajdzie, pytasz: „Jak oceniacie pilność?”	Głosują 1-5, uzasadniają.
Demo WU	8'	Offline film: Windows Update > pokaż KB i datę „Patch Tuesday”.	Wypisują klucz: severity + restart.
GPO live	15'	gpedit.msc → Computer Config → Windows → Security → Password Policy → Minimum length 12. Następnie gpupdate /force.	Logują test-userem, widzą odmowę prostego hasła.

Rollback	10'	Dyskusja scenki: „Patch psuje drukarki". Checklist: snapshot, staging, maintenance window.	Zaznaczają w arkuszu, który krok by dopisali (np. *dry-run*).
Podsum.	6'	Na tablicy „Patch-flow": *Info* → *Test VM* → *Snapshot OK* → *Prod* → *Monitor* → *Rollback?*	Łączą strzałkami etapy we własnym notesie.

5 | Pytania do dyskusji

1. Dlaczego **nie** instalować łatki „na żywo" na serwerze plików o 9:00?
2. Co sprawdzić *po* instalacji, zanim ogłosisz sukces?

6 | Ratunkowe wskazówki

- **Brak domeny** → robimy Local Security Policy; zasada podobna.
- **Update offline** → użyj wusa /quiet /norestart z paczką *.msu*.

7 | Dodatkowe źródła

- Microsoft „Security Update Guide" – filtrowanie po CVSS.
- CIS Benchmark *Windows 10* – rozdział „Account Policies".

LEKCJA 4 – „Ostatnia linia – Jump Server i Endpoint Security"

1 | Cele lekcji

Uczeń:

1. Konfiguruje dostęp SSH z kluczem do **Jump Servera** i łączy się z serwerem prod.
2. Wymienia trzy funkcje EDR i interpretuje prosty alert.
3. W grupie tworzy mini-projekt hardeningu szkolnej sieci (1 strona PDF).

2 | Czas trwania

45 min

3 | Potrzebne materiały

Narzędzie	**Rola**
VM „Jump” Ubuntu 22 + OpenSSH	bastion
VM „Prod1” w oddzielnym VLAN-ie	cel
Elastic Agent demo lub wideo	EDR
Szablon PDF „Plan Hardeningu”	projekt grupowy

4 | Przebieg zajęć

Krok	Czas	Działania	Uczniowie
Kontekst	5'	Rysujesz diagram: Admin PC → Jump (10.0.0.5) → Prod1 (10.1.0.10).	Upewniają się, że tylko Jump ma dostęp do Prod1.
Klucze SSH	12'	ssh-keygen -t ed25519 -f ~/.ssh/jump_key → ssh-copy-id -i jump_key.pub admin@10.0.0.5. Zwróć uwagę na *PasswordAuthentication no*.	Powtarzają, łączą się bez hasła, próbują bez klucza (odrzucone).
Tunelowanie	6'	ssh -J admin@10.0.0.5 admin@10.1.0.10. Podkreśl, że prod nie jest wystawiony „na świat”.	Testują uname -n na Prod1, sprawdzają brak otwartego SSH z zewnątrz (nmap).
Endpoint Security	10'	W konsoli Elastic Security pokazujesz alert „Suspicious PowerShell”. Omawiasz pola: timestamp, host, action.	W duo notują 2 opcje reakcji: isolate host / kill process.
Projekt	10'	Grupy 4-os.: wypełniają PDF (*obszar* + *technika* + *kryterium sukcesu* + *kto odpowiada*).	Po lekcji oddają na Teams / Classroom.

Finał	2'	Motto: „Hardening ≠ jednorazowa kampania – to ciągły cykl oceny, wdrożenia i weryfikacji.”	Brawa dla siebie 😉

5 | Pytania do dyskusji

- Jak zabezpieczyć Jump Server, aby sam nie stał się „single point of failure”?
- Czym różni się alert EDR od klasycznego wykrycia AV?

6 | Ratunkowe wskazówki

- **Brak VM** → pokaz slajdów + gotowy plik PCAP z tunelowania.
- **EDR demo offline** → wideo 3 minuty, potem rozpakowany JSON alertu do analizy ręcznej.

7 | Dodatkowe źródła

- SANS Whitepaper „DNS Sinkhole 101”.
- man iptables – sekcja *Target Extensions*.